ITS Technical Bulletin 174
SECURITY CONSIDERATIONS FOR CONTROL-M

Issued Date: December 16, 1993
Effective Date: December 30, 1993
Section/Groups: Software Support
Submitted By:
Approved By: Dave Jeffs

General Information:

Control-M security is accomplished through an external security interface. All authorization checking is done through calls to ACF2.

In order to establish a Control-M environment and administer proper access controls the five areas outlined in this technical bulletin must be addressed.

The naming standards outlined herein are for administration, security, and System Managed Storage (SMS) purposes. If these standards are not adhered to in all future Control-M definitions ITS will not provide support for scheduling functions. (Existing Control-M definitions that were created as a result of the conversion from CA7 and do not conform with these standards will be exempt until they are migrated into new libraries.)

1. Control-M Monitor (Online Environment)

Access to the Control-M online environment (ISPF Local option L.CTM) requires access granted by the ACF2 resource rule $$IOAONLINE.I2 Security access to this resource will be administered by ITS Security. Requests for access to the Control-M Monitor will be accepted only through authorized agency security administrators.

2. Control-M Monitor (Active Environment)

Access to the Control-M monitor (option 3 from the Control-M primary option menu) requires additional access granted by the ACF2 resource rule $$CTMPNL3.I2 Security access to this resource will be administered by ITS Security. Requests for access to option 3 will be accepted only through authorized agency security administrators.

3. Schedule Owners

Each Control-M schedule definition has an "OWNER" field that names the ACF2 LogonID to be used when the job is submitted. JCL for jobs submitted through Control-M must not have LogonID or Password cards. The ACF2 LogonID must be established so that it may only be submitted through Control-M. Have your agency security administrator contact ITS security for the proper definitions.

Once a proper LogonID is established its use may be secured by the ACF2 resource rule $SUBMIT.owner (type R-IOA). There must be a separate ACF2 rule for each OWNER.

Currently access granted by a $SUBMIT.owner rule will allow all scheduling functions for jobs having that owner.

EXTENDING SECURITY: Extended security definitions (not now in effect) can be defined to control functions such as; Browsing SYSOUT, Showing Job Statistics, showing the log, holding jobs, rerunning jobs, changing jobs in the active queue, deleting jobs, editing JCL for jobs etc... Agencies may find it necessary to restrict certain functions to control or on-call people while allowing general access to other scheduling functions.

4. Output Conditions (OUT Conditions)

Most Control-M jobs will issue Output Conditions. To authorize output conditions to be issued Control-M will check the ACF2 rule $$IOARES.I2.table-name_job-name (type R-IOA)

To conform with security and naming standards all table names must begin with an authorized two character agency code.

EXTENDING SECURITY: Extended security definitions (not now in effect) may be defined so that agencies may restrict certain functions to control or on-call people while allowing general access to other scheduling functions.

5. Scheduling Datasets.

To create new schedule definitions or to modify existing schedules ACF2 access to the proper datasets is needed. All new Control-M Datasets must follow these naming standards.

Scheduling Library = agency-code.application-name.CTMSCHED
JCL Library = agency-code.application-name.CTMJCL
Documentation Lib. = agency-code.application-name.CTMDOC
Calendar Library = agency-code.application-name.CTMCAL
Parameter Library = agency-code.application-name.CTMPARM